BAB II

TINJAUAN PUSTAKA

2.1 Profil Tempat Kerja Praktek

2.1.1 Sejarah Instansi

B4T didirikan pada tahun 1909 di Batavia (Jakarta sekarang) oleh pemerintahan Hindia Belanda dengan nama Laboraturium Voor Metal Onderzoek dan berada di bawah naungan Brugelizke Openbake Warken (Departemen Pekerjaan Umum sekarang).

Pada tahun 1912 diperluas menjadi Laboraturium Voor Material Onderzoek. Yang semula balai ini hanya mengurus benda-benda metal diperluas dengan benda material lainya.

Pada tahun 1921 lokasi balai dipindahkan ke Bandung. Tepat nya ke lokasi Technische Hogescholl (Institut Teknologi Badung sekarang). Pada tahun 1934 kedudukan balai berindah ke naungan Van Ekonomische (Departemen Perekonomian dan Pendagangan).

Pada tahun 1942 dibawah kekuasaan Jepang balai berubah nama menjadi Laboraturium Zeiro Sikendya dan kemudian beruba lagi menjadi Laboraturium Kogio Sikendya.

Tahun 1945 Indonesia merdeka dan balai ini kembali berubah nama menjadi Balai Penyelidikan Bahan-bahan yang berkedudukan dibawah kementrian Kemakmuran. Pada periode tahun 1952 – 1960 balai ini dua kali beralih naungan, yaitu dari Kementrian Perekonomian ke Kementrian Perindrustian. Pada tahun 1961 balai ini menempati Jalan Sangkuriang Bandung dengan nama Balai Penelitian Bahan-bahan. Pada tahun 1963 kedudukan balai berada di bawah Perindustrian Rakyat.

Tahun 1971 kedudukan balai berada di bawah naungan Lembaga Penelitian dan Pendidikan Industri. Pada tahun 1974 kedudukan balai berada di bawah Puslitbang Industri. Pada tahun 1974 kedudukan balai berda dibawah Puslitbang Industri Logam dan Mesin Departemen Perindustrian.

Tahun 1980 kedudukan balai dibawah Badan Litbang Industru Departemen Perindustran dan berubah nama menjadi Balai besar Penelitian dan Pengembangan Industri Bahan dan Barang Teknik. Dan pada akhir taun 2002 balai ini berubah nama menjadi Balai Besar Bahan dan Barang Teknik yang disingkat dengan B4T dan dipakai hingga sekarang.

Balai besar Bahan dan Barang Teknik (B4T) beralamat di Jalan Sangkuriang No. 14 Bandung 40135. Telp. 022 – 2504088, 2504828, 2510682. Fax 022 – 2502027. Website : www.b4t.go.id dan e-mail : info@b4t.go.id.

2.1.2 Logo Instansi



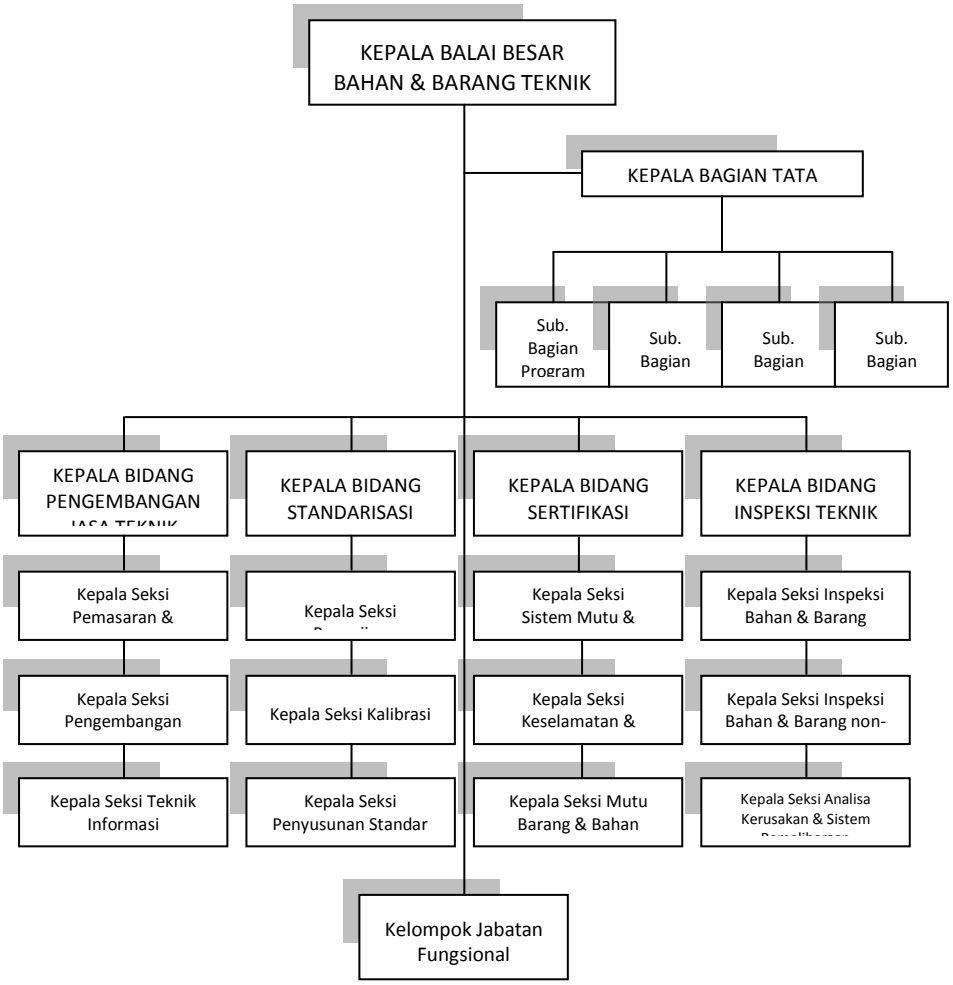
Gambar 1 : Logo Instansi B4T

2.1.3 Badan Hukum Instansi

Balai besar Bahan dan Barang Teknik (B4T) merupakan balai resmi pemerintah yang berada di bawah naungan Badan Pengkajian Kebijakan Iklim dan Mutu Industri, Kementrian Perindustrian. Badan hukum oleh Menteri Perindustrian Republik Indonesia Nomor : 43/M-IND/PER/6/2006 Tentang organisasi dan tata kerja Balai Besar Bahan dan Barang Teknik.

Struktur Organisasi dan Job Description

Berikut gambar struktur organisasi B4T :



Gambar 2 : Struktur Organisasi B4T

Berikut ini merupakan deskripsi pekerjaan dari struktur organisasi sertifikasi di B4T sesuai dengan jabatanya masing-masing.

1. Kepala B4T

   Mengerjakan hal-hal sebagai berikut :

a. Sebagai pimpinan di B4T.
b. Mengawasi jalanya aktivitas di B4T.
c. Menetapkan tugas dari kepala bidang yang ada.
d. Mengawasi dan mengkoordinir kegiatan-kegiatan dari setiap kepala bidang yang ada.

2. Kepala bidang Sertifikasi

   Mengerjakan hal-hal sebagai berikut :

a. Sebagai pemimpin di divisi sertifikasi.
b. Menetapkan kegiatan sertifikasi.
c. Menyetujui semua dokumen yang masuk ke divisi sertifikasi.
d. Menerbitkan sertifikasi.

3. Kepala seksi Pemasaran dan Kerjasama

   Mengerjakan hal-hal sebagai berikut :

a. Membicarakan proses sertifikasi dengan perusahaan.
b. Mengawasi kerja tim sertifikasi.
c. Mengecek data perusahaan yang di sertifikasi.

4. Kepala Seksi Informasi

   Mengerjakan hal-hal sebagai berikut :

a. Mengawasi jaringan server di bagian sertifikasi.
b. Mengawasi semua sistem yang berjalan di bagian sertifikasi.
c. Admin di sistem sertifikasi.

2.2 Landasan Teori

Selama pelaksanaan kerja praktek di Balai Besar Bahan dan Barang Teknik (B4T), kelompok kerja praktek menggunakan pengetahuan yang diperoleh selama dalam masa perkuliahan sebgai landasan teori dalam pengembangan system intranet dan internet di B4T dan beberapa pengetahuan baru yang didapat pada saat pelaksanaan kerja praktek berlangsung.

2.2.1 Pengertian Jaringan Komputer

Jaringan komputer merupakan sekelompok komputer otonom yang saling dihubungkan satu sama lainnya, menggunakan suatu media dan protokol komunikasi tertentu, sehingga dapat saling berbagi data dan informasi. Jaringan komputer memungkinkan terjadinya komunikasi yang lebih efisien antar pemakai (*mail* dan *teleconference*).

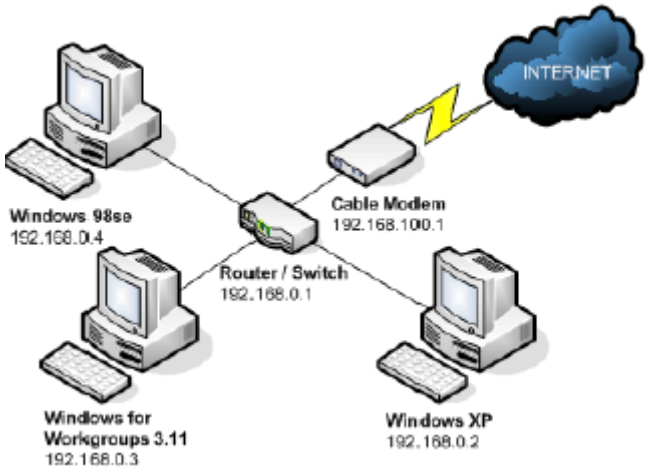
Jaringan komputer adalah sekelompok komputer otonom yang saling menggunakan protokol komunikasi melalui media komunikasi sehingga dapat berbagai data, informasi, program aplikasi dan perangkat keras seperti *printer, scanner,* CD-Drive maupun *harddisk* serta memungkinkan komunikasi secara elektronik.

Sedangkan pada aplikasi *home user*, memungkinkan komunikasi antar pengguna lebih efisien (chat), interaktif *entertainment* lebih multimedia (games, video, dan lain-lain).

Klasifikasi Jaringan Komputer :

1. LAN *(Local Area Network)*

   Jaringan komputer yang saling terhubung ke suatu komputer server dengan menggunakan topologi tertentu, biasanya digunakan dalam kawasan satu gedung atau kawasan yang jaraknya tidak lebih dari 1 km.

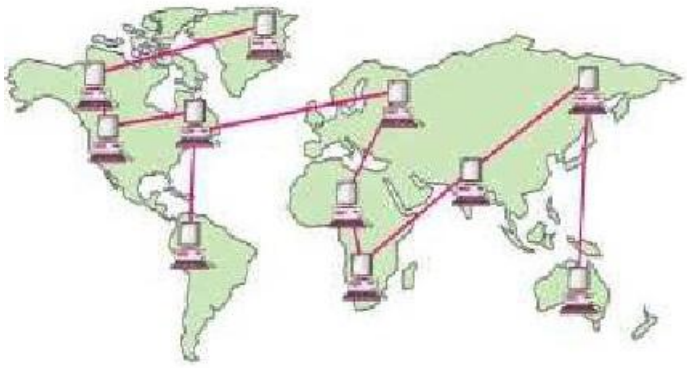


Gambar 3 LAN (*Local Area Network)* – sumber :

www.garethjmsaunders.co.uk

2. WAN (*Wide Area Network)*

   Jaringan komputer yang menghubungkan banyak LAN ke dalam suatu jaringan terpadu, antara satu jaringan dengan jaringan lain dapat berjarak ribuan kilometer atau terpisahkan letak geografi dengan menggunakan metode komunikasi tertentu.



Gambar 4 WAN *(Wide Area Network)* – sumber :

www.cisco.com

Secara garis besar ada beberapa tahapan dalam membangun jaringan LAN, diantaranya :

1. Menentukan teknologi tipe jaringannya (*Ethernet, Fast Ethernet, Token Ring*, FDDI).
2. Memilih model perkabelan (*Fiber, UTP, Coaxial*).
3. Menentukan teknologi *Client Server* atau *Peer to Peer.*
4. Memilih sistem operasi server (Windows NTS, 2000, XP, atau Linux).

2.2.2 Model Konektifitas Jaringan Komputer

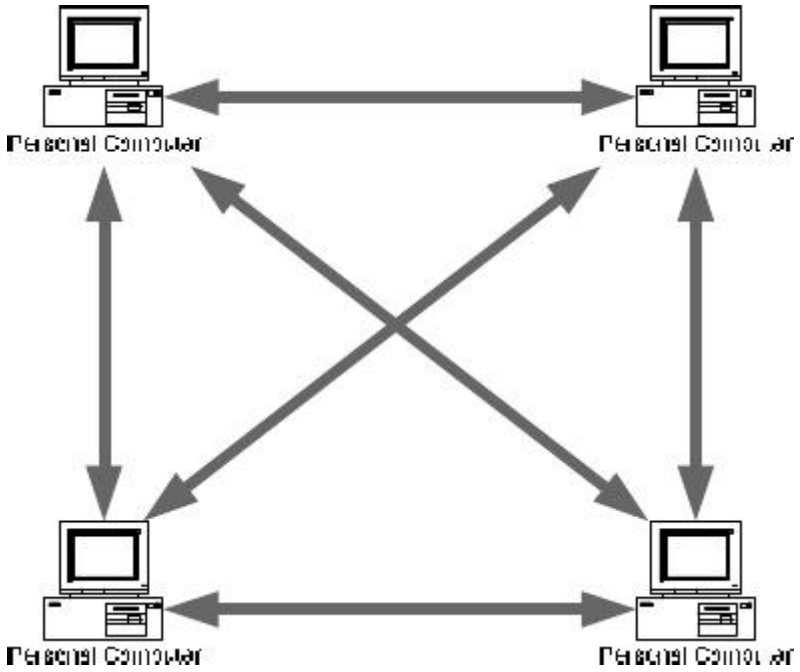
Model konektifitas jaringan komputer diantaranya adalah sebagai berikut:

1. Model *Peer to Peer*

   Pada model ini semua komputer atau mesin yang terhubung mempunyai kedudukan dan fungsi yang sama. Dalam hal ini tidak ada komputer yang menjadi pengendali utama. Setiap host dalam model ini

dapat menawarkan layanan ke *peer* yang lain dan juga dapat mengambil layanan dari *peer* lain.

Model ini cocok untuk jaringan kecil. Fasilitas yang tersedia untuk mode ini adalah berbagi file dan berbagai *printer* serta piranti lainnya.



Gambar 5 Model Jaringan Peer to Peer

2. Model *Client Server*

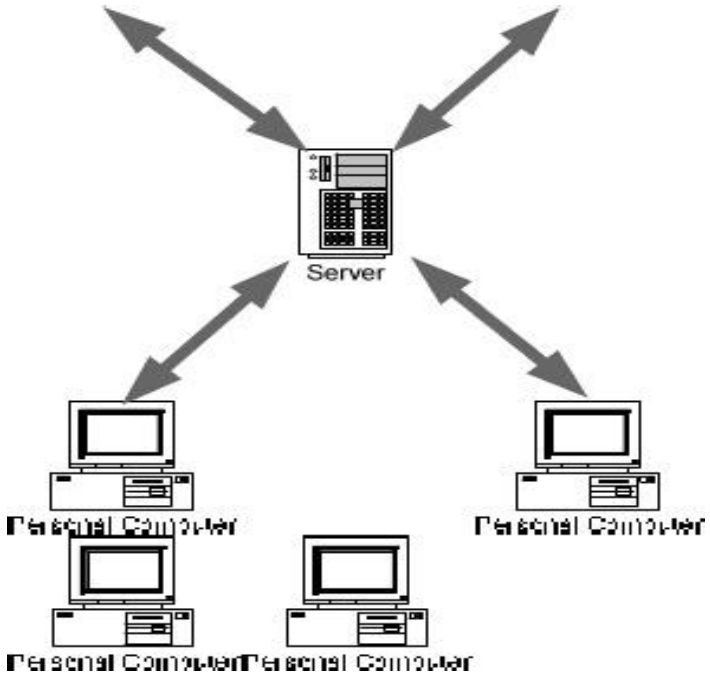
Pada model ini terdapat dua atau lebih mesin yang bertindak sebagai *file server* dan mesin lainnya sebagai *client.* Model ini memisahkan secara jelas mana yang dapat memberikan layanan jaringan *(server)* dan mana yang hanya menerima layanan (*client*).

Beberapa komputer di *setup* sebagai *server* yang memberikan segala sumber daya *(resource)* dari jaringan seperti *printer, modem,* dan lain-lain kepada komputer lain yang terkoneksi ke jaringan yang berfungsi sebagai *client.*

Untuk dapat berkomunikasi antara *server* dan *client, server* menggunakan aplikasi jaringan yang disebut *server program*, sementara

client menggunakan *client* program untuk berkomunikasi dengan *server program* pada *server*.

Komunikasi pada *client-server* pada umumnya berbentuk pesan permintaan untuk melaksanakan berbagai pekerjaan dari *client* kepada *server*. Setelah *server* melaksanakan tugasnya, kemudian hasilnya akan dikirim kembali kepada *client.*



Gambar 6 Model Jaringan Client Server

2.2.3 Intrusion Detection System (IDS)

Instrusion Detection System (IDS) adalah sebuah aplikasi perangkat lunak atau keras yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah system jaringan. IDS dapat melakukan inspeksi lalu lintas inbound maupun outbound dalah sebuah system atau jaringan, melakukan analisis dan mencari bukti dari percobaan instrusi (penyusupan).

Ada dua jenis IDS, yaitu:

1. Network-based Intrusion Detection System (NIDS).

   Semua lalu lintas yang mengalir ke sebiah jaringan akan dianalisis untuk mencari apakah ada percobaan serangan atau penyusupan ke dalam sistem jaringan. NIDS umumnya terletak di dalam segmen jaringan penting di mana server berada atau terdapat pada "pintu masuk" jaringan. Kelemahan NIDS adalah bahwa NIDS agak rumit diimplementasikan dalam sebuah jaringan yang menggunakan switch Ethernet, meskipun beberapa *vendor* switch Ethernet sekarang telah menerapkan fungsi IDS di dalam *switch* buatannya untuk memonitor port atau koleksi.

2. Host-based Intrusion Detection System (HIDS)

   Aktivitas sebuah *host* jaringan individual akan dipantau apalaj terjadi sebuah percobaan serangan atau penyusupan ke dalamnya atau tidak. HIDS seringnya diletakkan pada server-server kritis di jaringan, seperti halnya *firewall, web server,* atai server yang terkoneksi ke Internet.

Kebanyakan produk IDS merupakan sistem yang bersifat pasif, mengingat tugasnya hanyalah mendeteksi intrusi yang terjadi dan memberikan peringatan kepada administrator jaringan bahwa mungkin ada serangan atau gangguan terhadap jaringan.

Akhir-akhir ini, bebrapa *vendor* juga mengembangkan IDS yang bersifat aktif yang dapat melakukan beberapa tugas untuk melindungi host atau jaringan dari serangan ketika terdeteksi, seperti halnya menutup beberapa *port* atau memblokis beberapa alamat IP. Produk seperti ini umumnya disebut sebagai *Intrusion Prevention System* (IPS). Beberrapa

produk IDS juga menggabungkan kemampuan yang dimiliki oleh HIDS dan NIDS, yang kemudian fisebut sebagai sistem hybrid (*Hybrid Intrusion Detection System).*

Ada beberapa cara bagaimana IDS bekerja. Cara yang paling popular adalah dengan menggunakan pendeteksian berbasis *signature* (seperti halnya yang dilakukan oleh beberapa antivirus), yang melibatkan pencocokan lalu lintas jaringan dengan basis data yang berisis cara-cara serangan dan penyusupan yang sering dilakukan oleh penyerang. Sama seperti halnya antivirus, jenis ini membutuhkan pembaruan terhadap data *signature* IDS yang bersangkutan.

Metode selanjutnya adalah dengan mendeteksi adanya anomali, yang disebut sebagai *Anomalu-based* IDS. Jenis ini melibatkan pola lalu lintas yang mungkin merupakan sebuah serangan yang sedang dilakukan oleh penyerang. Umumnya, dilakukan dengan menggunakan teknik statistic untuk membandingkan lalu lintas yang sedang dipantau dengan lalu lintas normal yang biasa terjadi. Metode ini menawarkan kelebihan dibandingkan *signatute-based* IDS, yakni ia dapat mendeteksi bentuk serangan yang baru dan belum terdapat di dalam basis data *signature* IDS. Kelemahannya adalah jenis ini sering mengeluarkan pesan *fulse positive*. Sehingga tugas *administrator* menjadi lebih rumit, dengan harus memilah-milah mana yang merupakan serang yang sebenarnya dari banyaknya laporan *fulse positive* yang muncul.

Teknik lainnya yang digunakan adalah dengan memantau berkas-berkas sistem operasi, yakni dengan cara melihat apakah ada percobaan

untuk mengubah beberapa berkas sistem operasi, utamanya berkas log. Teknik ini seringnya diimplementasikan di dalam HIDS, selain tentunya melakukan pemindaian terhadap log sistem untuk memantau apakah terjadi kejadian yang tidak biasa.

2.2.4 Intranet

Intranet adalah sebuah jaringan komputer berbasis protokol TCP/IP seperti internet hanya saja digunakan dalam internal perusahaan, kantor, bahkan warung internet (WARNET) pun dapat di kategorikan Intranet. Antar Intranet dapat saling berkomunikasi satu dengan lainnya melalui sambungan Internet yang memberikan tulang punggung komunikasi jarak jauh. Akan tetapi sebetulnya sebuah Intranet tidak perlu sambungan luar ke Internet untuk berfungsi secara benar. Intranet menggunakan semua protocol TCP/IP dan aplikasinya sehingga kita memiliki "*private*" Internet.

2.2.5 Internet

Internet adalah jaringan komputer yang luas dan besar yang mendunia, yaitu menghubungkan pemakai computer dari suatu Negara ke Negara lain di seluruh dunia, dimana di dalamnya terdapat berbagai sumber daya informasi dari mulai yang statis hingga yang dinamis dan interaktif.

2.2.6 Proxy Server

Sebuah fasilitas untuk menghubungkan diri ke internet secara bersama-sama. Memenuhi permintaan user untuk layanan internetn (http, FTP, Telnet) dan mengirimkannya sesuai dengan kebijakan. Bertindak sebagai *gateway* menuju layanan. Mewakili paket data dari dalam dan dari luar.

Menangani semua komunikasi internet *eksternal*. Bertindak sebagai *gateway* antara mesin *internal* dan *eksternal*. Proxy server mengevaluasi dan mengontrol permintaan dari *client*, jika sesuai *policy* dilewatkan jika tidak di *deny/drop*. Menggunakan metode NAT. Memerikas isi paket.

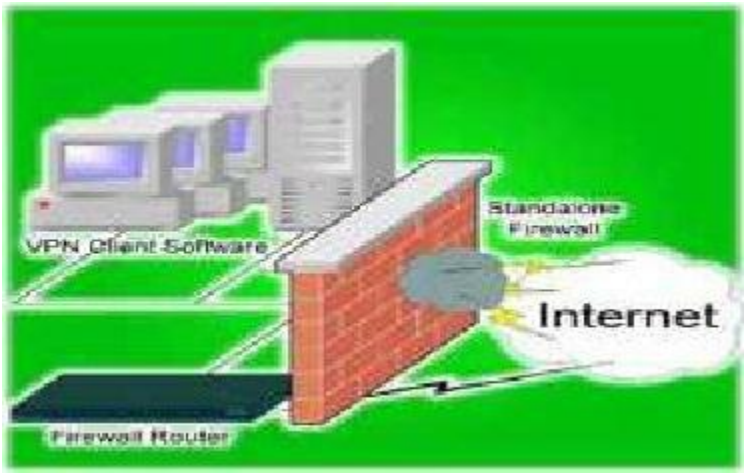
2.2.7 Firewall

Sistem keamanan yang menggunakan *device* atau sistem yang diletakkan di dua jaringan dengan fungsi utama melakukan *filtering* terhadap akses yang akan masuk.

Berupa seperangkat *hardware* atau *software*, bisa juga berupa seperangkat aturan dan prosedur yang diterapkan oleh organisasi. *Firewall* juga dapat disebut sebagai sistem atau perangkat yang mengizinkan lalu lintas jaringan yang dianggapnya aman untuk melaluinya dan mencegah lau lintas jaringan yang tidak aman.

Umumnya *firewall* diimplementasikan dalam sebuah mesin terdedikasi, yang berjalan pada pintu gerbang (*gateway)* anatara jaringan lokal dan jaringan lainnya. *Firewall* juga umumnya digunakan untuk mengontrol akses terahadap siapa saja yang memiliki akses terhadap jaringan pribadi dari hak luar.

Saat ini, istilah *firewall* menjadi *generic* yang merujuk pada sistem yang mengatur komunikasi antara dua jaringan yang berbeda.



Gambar 7 Skema Firewall

2.2.8 Gateway

Gateway merupakan pintu gerbang sebagi keluar – masuknya paket data dari local network menuju outer network agar client pada local network dapat berkomunikasi dengan internet. Router dapat diseting menjadi Gateway dimana ia menjadi penghubung antara jaringan local dan jaringan luar.

2.2.9 Pengertian Sistem Operasi

Sistem operasi adalah sekumpulan rutin perangkat lunak yang berada diantara program aplikasi dan perangkat. Sistem operasi memiliki tugas yaitu mengelola seluruh sumber daya sistem komputer dan sebagai penyedia layanan.

Sistem operasi menyediakan Sistem Call (berupa fungsi-fungsi atau API-*Application Progamming Interface*). Sistem Call ini memberikan abstraksi tingkat tinggi mesin untuk pemrograman. Sistem Call berfungsi menghindarakn kompleksitas pemrograman dengan memberi sekumpulan intruksi yang lebih mudah dan nyaman, sistem operasi juga sebagai basis

untuk program lain dimana program aplikasi dijalankan diatas sistem operasi, program-program itu memanfaatkan sumber daya sistem komputer dengan cara meminta layanan sistem operasi mengendalikan sumber daya untuk aplikasi sehingga pengguna sumber daya sistem komputer dapat dilakukan secara benar dan efisien.

Sistem operasi yang dikenal antara lain :

1. Windows (95, 98, ME, 2000, VISTA, SERVER, Windows7).
2. Linux (Red Hat, Slackware, Ubuntu, Fedora, Mikrotik, Debian, OpenSUSE).
3. UNIX
4. FreeBSD (Berkley Software Distribution)
5. SUN (SOLARIS).
6. DOS (MS-DOS)
7. Machintosh (MAC OS, MAC OSX).

2.2.10 Mikrotik

Mikrotik adalah system operasi independen berbasiskan Linux dan perangkat lunak yang dapat digunakan untuk menjadikan computer anda menjadi router network yang handal mencakup sebagai fitur yang dibuat untuk *ip network* dan jaringan wireless.

2.2.11 Internet Protocol (IP)

Internet Protocol (IP) adalah metode atau protocol untuk mengirimkan data ke Internet. Setiap computer (host) dalam internet setidaknya harus mempunyai sebuah alamat IP yang unik untuk mengindentifikasikan komputer tersebut terhadap host yang lain.

2.2.12 Domain Name Service (DNS)

Domain Name Service (DNS) adalah suatu aplikasi penyimpanan dan pengambilan tentang nama host dan alamat ip di dalam suatu database yang terdistribusi, yang berfungsi menerjemahkan alamat ip komputer dengan alamat yang lebih manusiawi atau bahasa lainya "*humanable*".